Standards Landscape and ICT SCRM Study Period

Nadya Bartol

September 28, 2010

Booz | Allen | Hamilton

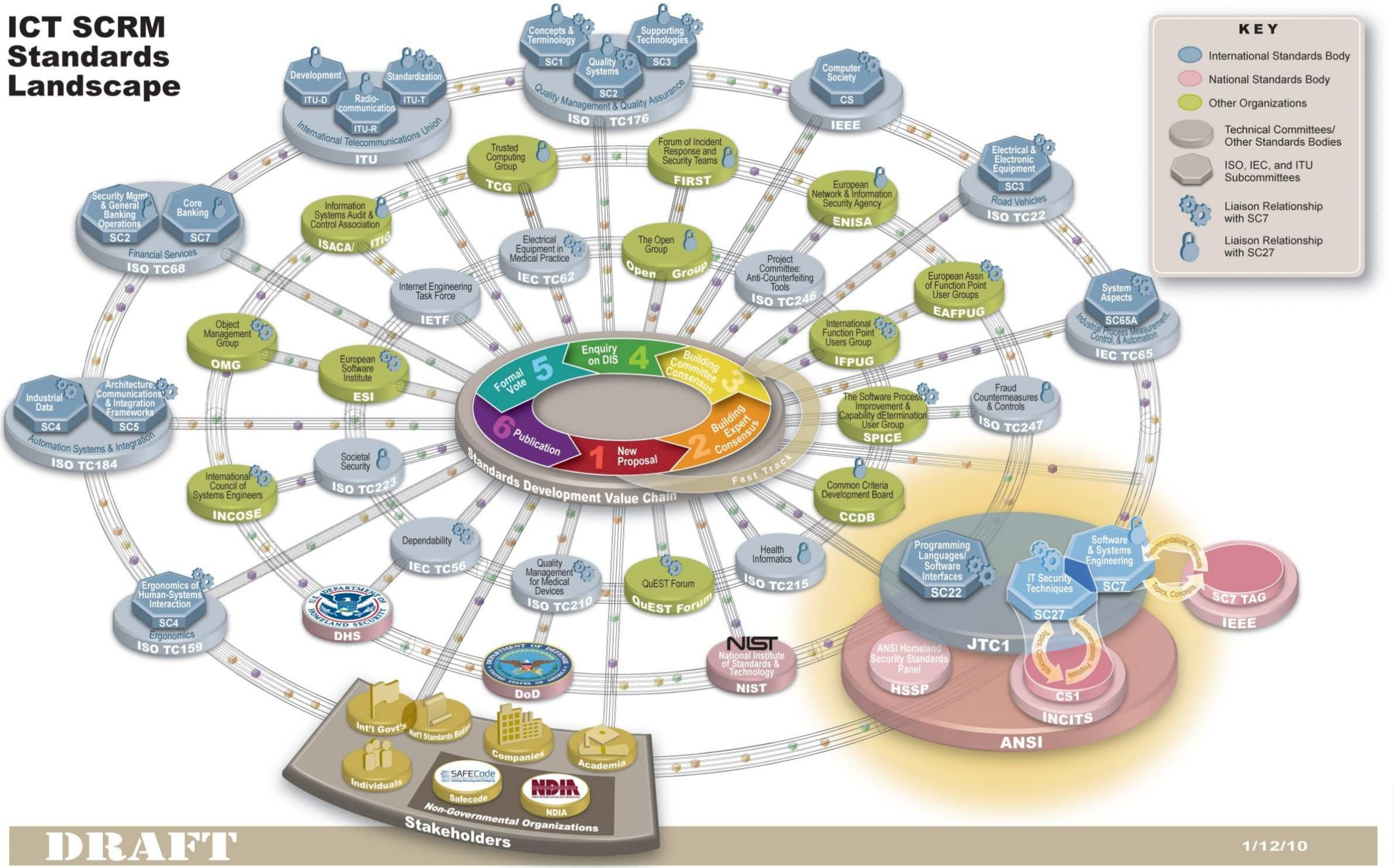
Table Of Contents

- Standards Landscape
- Study period scope
- Scope of problem
- Contributions and other sources
- Related efforts
- Conclusions and recommendations

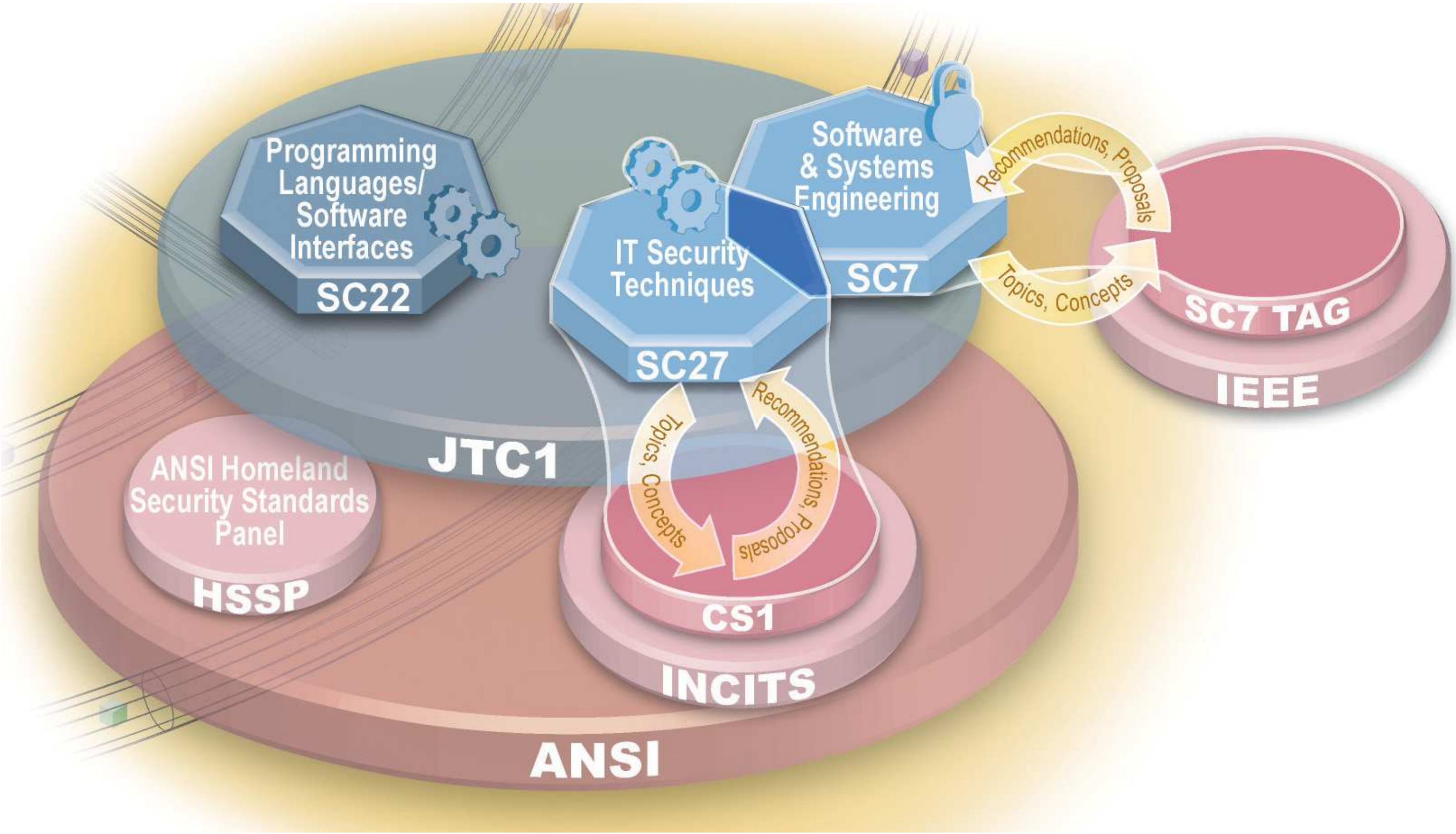
ICT Supply Chain Assurance Standards Landscape is Rather Complex

- ICT Supply Chain Assurance incorporates practices from
  - Information security
  - Software Assurance
  - System and software engineering
  - Supply chain and logistics
  - Other fields
- Currently there is no single standard addressing ICT Supply Chain Assurance
- However there are LOTS of standards that can be
  - Updated to integrate aspects of and pointers to ICT Supply Chain Assurance
  - Used to apply ICT Supply Chain Assurance techniques
- Furthermore, there are emerging government and industry practices that can be leveraged to enhance content of existing standards or develop specific new standard

The Landscape


ICT SCRM Standards Landscape
KEY
International Standards Body
National Standards Body
Other Organizations
Technical Committees/ Other Standards Bodies
ISO, IEC, and ITU Subcommittees
Liaison Relationship with SC7
Liaison Relationship with SC27
Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International Telecommunications Union
ITU
Concepts & Terminology
SC1
Quality Systems
SC2
Supporting Technologies
SC3
Quality Management & Quality Assurance
ISO TC176
Computer Society
CS
IEEE
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
System Aspects
SC65A
Industrial Process Measurement, Control, & Automation
IEC TC65
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
Industrial Data
SC4
Architecture, Communications, & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
Trusted Computing Group
TCG
Forum of Incident Response and Security Teams
FIRST
European Network & Information Security Agency
ENISA
Information Systems Audit & Control Association
ISACA/ITIG
Electrical Equipment in Medical Practice
IEC TC62
The Open Group
Open Group
Project Committee: Anti-Counterfeiting Tools
ISO TC246
European Assn of Function Point User Groups
EAFPUG
Internet Engineering Task Force
IETF
Object Management Group
OMG
European Software Institute
ESI
International Function Point Users Group
IFPUG
The Software Process Improvement & Capability dEtermination User Group
SPICE
Fraud Countermeasures & Controls
ISO TC247
Societal Security
ISO TC223
International Council of Systems Engineers
INCOSE
Common Criteria Development Board
CCDB
Dependability
IEC TC56
Quality Management for Medical Devices
ISO TC210
QuEST Forum
QuEST Forum
Health Informatics
ISO TC215
DHS
DoD
NIST
National Institute of Standards & Technology
NIST
1 New Proposal
2 Building Expert Consensus
3 Building Committee Consensus
4 Enquiry on DIS
5 Formal Vote
6 Publication
Fast Track
Standards Development Value Chain
Programming Languages/ Software Interfaces
SC22
Software & Systems Engineering
SC7
IT Security Techniques
SC27
JTC1
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI
Int'l Govt's
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
Non-Governmental Organizations
Stakeholders
DRAFT
1/12/10

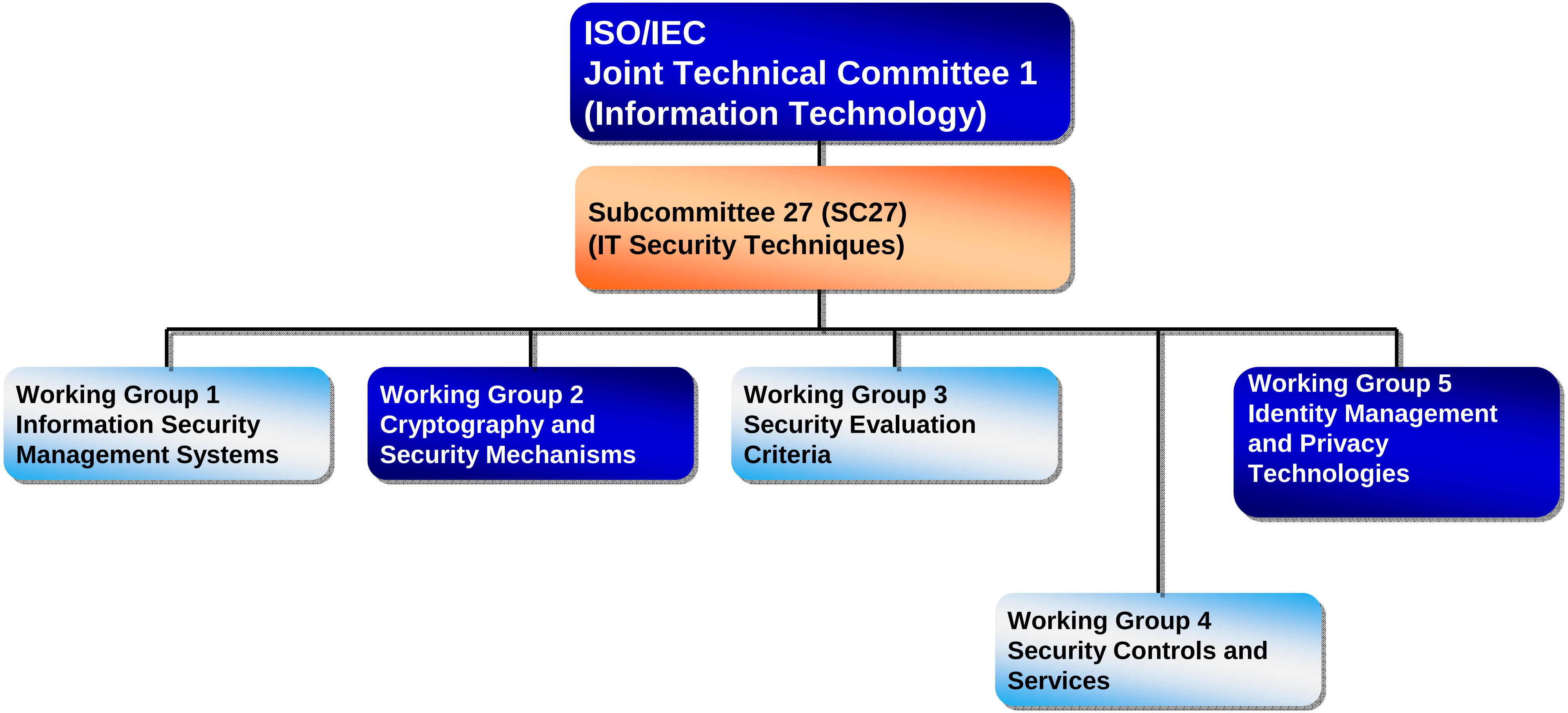
ISO/IEC JTC1 SC7 and ISO/IEC JTC1 SC27 have a substantial number of relevant standards


Programming Languages/ Software Interfaces
SC22
IT Security Techniques
SC27
Software & Systems Engineering
SC7
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
JTC1
Topics, Concepts
Recommendations, Proposals
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI

CS1 ICT SCRM Ad Hoc Group

- Established in February 2009
- Joint with SC7 TAG
- Substantial industry and government participation
- Contributed to several new and under revision standards
- Developed consensus-based USNB proposal for ICT Supply Chain Assurance Standard

ISO/IEC JTC1 SC27 focuses on IT Security Techniques



ISO/IEC
Joint Technical Committee 1
(Information Technology)

Subcommittee 27 (SC27)
(IT Security Techniques)

Working Group 1
Information Security
Management Systems

Working Group 2
Cryptography and
Security Mechanisms

Working Group 3
Security Evaluation
Criteria

Working Group 4
Security Controls and
Services

Working Group 5
Identity Management
and Privacy
Technologies

ICT Supply Chain Security Study Period

- Study Period was proposed by the US, with a draft New Work Item Proposal presented at the WG4 meeting
- WG4 approved a Study Period to address ICT SCRM with a title ICT Supply Chain Security (term Risk Management was challenging)
- Nadya Bartol was appointed a Rapporteur for the Study Period and is responsible for consolidating National Body comments and producing a report with a recommendation to be presented at the May 2010 meeting
- Anticipated result of the Study Period is a New Work Item Proposal to develop a new standard to address ICT SCRM or ICT Supply Chain Assurance
- US submitted a substantial contribution. In addition to DoD, NIST, Microsoft, Boeing, and SAFECode are interested in this work

Study Period Scope and Objectives

- Scope
  - Address specific IT security practices to help ICT product and service acquirers manage the risks to their ICT from the global supply chain
  - Define ICT supply chain and related assurance practices and describe ICT supply chain assurance practices throughout the lifecycle processes, as described in ISO/IEC 15288, System Lifecycle Processes and ISO/IEC 12207, Software Lifecycle Processes
  - Address basic concepts for increasing supply chain assurance
  - Discuss specific techniques focused on addressing risks to ICT throughout global supply chain
  - Provide references to other international standards and technical reports that address existing practices and techniques that can be applied to supply chain risk management
- Objectives
  - Scope the problem
  - Define audience
  - Propose options for intended outcome (e.g., IS vs. TR)
  - Identify related standardization efforts (published or currently under development)
- Time frame
  - Approved in Redmond, November 2009
  - Contributions received in April 2010 ahead of the Melaka meeting
  - Meet in Melaka to discuss contributions and chart the way forward

What is the Problem and Gaps We Are Trying to Address?

- Information and Communication Technology (ICT) products are assembled, built, and transported by multiple vendors around the world before they are acquired ***without the knowledge of the acquirer***

- Abundant opportunities exist for malicious actors to tamper with and sabotage products, ultimately compromising system integrity and operations ***evidenced by multiple recently publicized incidents*** (counterfeit hardware sold to government agencies)

- Organizations acquiring hardware, software, and services are not able to understand and manage the security risks associated with the use of these products and services

- Challenges range from poor acquirer practices to lack of transparency into the supply chain
  - Substantial number of organizations or people can “touch” an ICT product without being identified
  - No standardized methodology or lexicon exists for managing ICT supply chain risks
  - Poor ICT products and services acquisition practices contribute to acquirers’ lack of understanding what is in their supply chain
  - Counterfeit hardware and software proliferate
  - Acquirers do not have a framework to help enforce security and assurance compliance for vendors

Potential Benefits of Developing a Standard

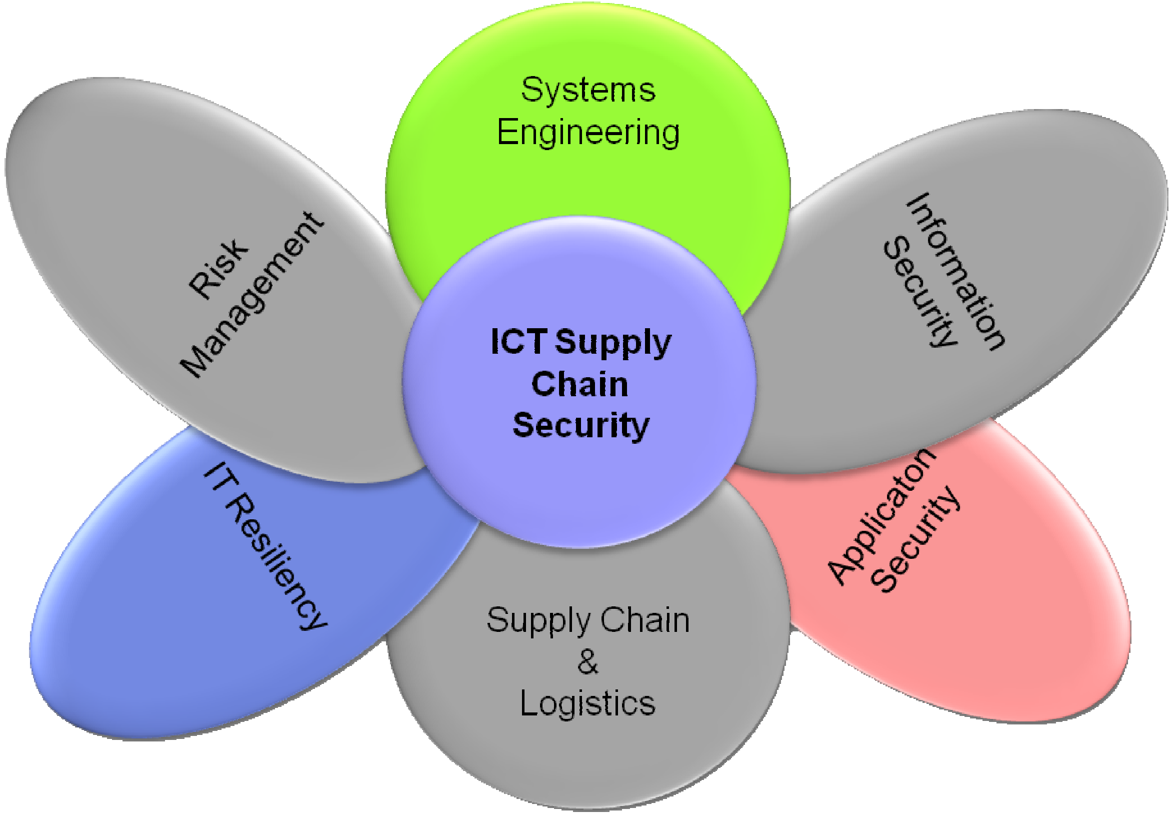
- Provide a common language for addressing the problem
  - Common lexicon
  - Recognizable process and techniques
  - Identify existing standards that can be leveraged as resources

- Provide a resource that would help acquirers ***articulate requirements*** to product and service providers and ***monitor implementation*** in a recognizable manner that is vetted internationally
  - Increase confidence in acquired products and services from security risk point of view
  - Create a common language to articulate expectations regarding security risks associated with product and service acquisition

- Provide a resource that would help product and service providers ***demonstrate responsible practices, regardless of where they are located***
  - Organizations that adopt the standard could gain competitive advantage by providing greater visibility for organizations acquiring products and services and therefore ***assurance that their products and services are less risky than their competition's***
  - Countries that adopt this standard can gain competitive advantage in being able to communicate to acquirers of outsourced products and services that they are able to ***decrease risks associated with ICT supply chain***

ICT Supply Chain Security Scope

- ICT Supply Chain Security intersects with many disciplines
- However, ICT Supply Chain Security focuses on a core group of practices that are specific to protecting ICT from ***security*** risks caused by the global/international supply chain
- The Study Period focuses on these core practices and acknowledges the relationship with other disciplines



Audience

- Acquirers and suppliers of ICT product would benefit from standardization in this area

  Acquirer – stakeholder that acquires or procures a product or service from a supplier [ISO/IEC 15288:2008]

  Supplier – organization or an individual that enters into an agreement with the acquirer for the supply of a product or service

  NOTE 1 Other terms commonly used for supplier are contractor, producer, seller or vendor.

  NOTE 2 The acquirer and the supplier may be part of the same organization. [ISO/IEC 15288]

Terms Currently Used to Address the Issue

- ICT Supply Chain Security
- ICT Supply Chain Integrity
- ICT Supply Chain Trust
- ICT Supply Chain Resilience
- Other?

Contributions and Other Sources

- National Body Contributions
- ISO 28001 and ISO 28002
- ENISA Studies
- Related existing and emerging ISO efforts

The Software Supply Chain Integrity Framework – SAFECode

- Describes software supply chain challenge
- Describes software assurance as a shared responsibility among suppliers (synonymous with vendors), service and/or solution providers, and customers encompassing three areas:
  - **Security: Security threats are anticipated** and addressed in the software's design, development and testing. This requires a focus on both quality aspects (e.g., "free from buffer overflows") and functional requirements (e.g., "passport numbers must be encrypted in the database")
  - **Authenticity: The software is not** counterfeit and customers are able to confirm that they have the real thing
  - **Integrity: The processes for sourcing,** creating and delivering software contain controls to enhance confidence that the software functions as the supplier intended
- Proposes a set of principles for designing software integrity controls

Software Supply Chain Security – Microsoft

- Customers are concerned about the origins of the code and is the software supply chain secure

- The real issue is not ***where*** but ***how*** the software is developed, specifically that the software is
  - Secure – security threats are anticipated by design, in development and deployment
  - Authentic – not counterfeit, and that it is easy to identify that it is what you requested
  - Sound – the origin of components is known and those with access are accountable

- Controls are required over software components
  - Received from suppliers
  - Developed in house
  - Delivered to customers

Draft NWIP, Security Guidelines for ICT Supply Chain Trust

- Scope – to address specific IT security practices to help ICT product and service acquirers gain visibility into the security risks caused by their supply chains.

- Proposed a multi-part standard to address the challenge due to the complexity of the problem and diverse audience for the standard:
  - Part 1: Overview and Concepts
  - Part 2: Risk Mitigations
  - Part 3: Implementation Guidance

- Identified relevant documents to be considered:
  - Management Systems: ISO/IEC 27000, ISMS and ISO 28000, Supply Chain Resiliency
  - Risk Management: ISO 31000, ISO/IEC 27005, and ISO/IEC 16085
  - Lifecycle Processes and Practices, software acquisition, and software assurance ISO/IEC/IEEE 15288 (systems), ISO/IEC/IEEE 12207 (software), IEEE 1062 (software acquisition), ISO/IEC15026 (software assurance)
  - Outsourcing: ISO/IEC 27036 and NWIP on Outsourcing in SC7

- Liaisons
  - US proposed a liaison with SC7
  - Discussion at the Melaka meeting identified additional liaisons with TC68, PC246, and TC8

15288/12207 Crosswalk

- ISO/IEC 15288 provides life cycle processes for any human-made system
- ISO/IEC 12207 specializes those processes for software-intensive systems and adds some software-specific processes
- Both standards provide acquisition and supply processes that are intended to be interpreted as a “conversation”, i.e. each activity of acquisition has a corresponding activity in supply
- The intent of providing this crosswalk was to
  - Demonstrate types of activities already described in international standards
  - Provide an example of language that could be useful
  - To ensure compatibility of the anticipated standard with existing system and software lifecycle processes standards

Results of Melaka Meeting

- US, Japan, and Malaysia participated
- Extended the Study Period
  - Give national bodies who could not make it an opportunity to present their view and participate in decision making
  - Solicit further contributions
  - Rapporteur to do further research
  - Request a half-day session for the Berlin meeting to have enough time to address
- Rapporteur to produce Study Period Report to include
  - NB contributions
  - ISO 28001/28002 summary and applicability
  - ENISA research
  - Other research that is relevant per Rapporteur
- Report content should address
  - Scope of the problem
  - Discussion and definition of a supply chain attack
  - Recommendation for the next steps
  - Potentially provide recommendations for other committees if identified issues are outside of scope for SC27 – for other SCs and TCs as well as a resource for other USNB as this issue may be important for countries (developing nations) basing their economic development on being ICT suppliers

ISO 28001 and 28002 (1 of 2)

- Originated from TC8 – Ships and Marine Technology
- **TC8 Scope:** Standardization of design, construction, structural elements, outfitting parts, equipment, methods and technology, and marine environmental matters, used in shipbuilding and the operation of ships, comprising sea-going ships, vessels for inland navigation, offshore structures, ship-to-shore interface and all other marine structures subject to IMO requirements
- Excluded:
  - **Electrical and electronic equipment on board ships and marine structures (IEC / TC 18 and IEC / TC 80)**
  - Internal combustion engines (ISO / TC 70)
  - Offshore structures for petroleum and natural gas industries, including procedures for assessment of the site specific application of mobile offshore drilling and accommodation units for the petroleum and natural gas industry (ISO / TC 67 / SC 7)
  - Steel and aluminum structures (ISO / TC 167)
  - Equipment and construction details of recreational craft and other small craft (not being lifeboats and lifesaving equipment) less than 24 meters in overall length (ISO / TC 188)
  - Sea bed mining
  - Equipment which is not specific for use on board ships and marine structures (e.g. pipes, steel wire ropes, etc.) and falling within the scope of particular ISO technical committees with which a regular mutual liaison must be maintained

ISO 28001 and 28002 (2 of 2)

- ISO/DIS 28001 – Security Management Systems for the Supply Chain – Best Practices for Implementing Supply Chain Security, Assessments, and Plans – Requirements and guidance
  - General management system for security of supply chain
  - Contains useful concepts (e.g., international supply chain vs. global supply chain) and definitions
  - Good source for referencing general supply chain security issues that are not ICT-related
- ISO 28002 – Resilience in the Supply Chain – Requirements with Guidance for Use
  - General resilience management system that includes supply chain
  - Mentions information security very few times
  - Provides a good reference for overall supply chain material

ISO 28001 and ISO 28002 provide sources of definitions and some lexicon, as well as the connection points for security to be referenced. However, they contain very few, if any references to information and IT security and alone are not sufficient for solving the ICT supply chain security problem.

ENISA Studies – Priorities for Research on Current and Emerging Network Technologies (PROCENT) Report (late 2009)

- Summarized the situation as follows:
  - Geographically distributed nature of the today's supply chain results in modern ICT systems, including platforms, network tools and their components, originating from a variety of locations
  - Different countries have differing requirements concerning various elements of the global supply chain, legal, export, regulatory and others, which have not yet been harmonized
  - Acquirers have difficulty associated with detecting and resolving defects when third-party components are used increasing the chances of data compromise and the time period required to recover and get operations back to normal
  - Increased opportunity for counterfeiting, cloning, reverse engineering, tampering, and the insertion of malicious components and misconfiguration that can result in new vulnerabilities or failure during normal operations

- Described the following key challenges that make achievement of supply chain integrity difficult:
  - Globally distributed and complex nature of supply chains: ICT components are manufactured in various countries around the world, and may be developed under contract by resellers and integrators then subsequently installed and operated by a variety of organizations
  - Lack of a common framework for ICT supply chain integrity: While good practices have been formulated by different industries, they are not always implemented consistently. This inconsistency makes it harder to ensure that the products as delivered have not been altered, counterfeited, or misconfigured
  - Absence of tools, processes, and controls to help measure confidence and verify integrity across the supply chain: Existing approaches and tools in many cases are not compatible with global supply chain dynamics
  - Available assurance evaluation frameworks are outdated or inadequate: Systems delivered to the end users cannot always be evaluated due to the lack of appropriate product evaluation models, methodologies, and tools
  - Lack of anti-counterfeiting/anti-tamper technology: Effective tools, techniques, and processes for detecting and defeating product counterfeiting and tampering are not yet available
  - Lack of a consistent approach for maintaining integrity controls throughout the product life cycle: Such controls are particularly lacking for use in dynamic environments, especially after the products have been delivered to their first owner

ENISA Studies – PROCENT Report

- ICT supply chain is susceptible to the following direct risks: ***supply chain attacks, insertion of malicious code, creation of counterfeited elements***

- Proposes the following key factors for managing supply chain integrity risks:
  - Clearly defining product and service requirements consistently carried through the whole supply chain from design, through production, delivery, purchase, installation, and maintenance of installed products and systems;
  - Existence of methodologies for evaluation and verification of components for compliance with upstream requirements;
  - Ability to evaluate provenance (the confirmed origin) and authenticity of the component parts, for both hardware and software, during assembly and installation, as well as through appropriate portions of the life of the product;
  - Measures to protect and maintain the integrity of systems, their configuration and operating parameters throughout their originally intended usage model

- Identifies opportunities for addressing the key challenge and/or vulnerabilities including
  - Improved and innovative models for establishing trust in suppliers and supplied products
  - Techniques for product evaluation and integrity checking
  - Study of good supply chain integrity practices
  - Solutions to detect and prevent counterfeiting
  - New approaches to supply chain security assurance
  - Inventory/configuration control and maintenance
  - Approaches for assessing global-scale supply chain integrity policy needs

PROCENT Report states that the subject should be treated on an international level, as the integrity of ICT supply chains is an issue crucial to all constituencies building, configuring and using ICT systems, including the private sector, academia, governments and international organizations.

ENISA Studies – ARECI report

- Availability and Robustness of Electronic Communications Infrastructures (ARECI) report published in 2007
- Identified the issue as follows:
  - the speed at which the shift to outsourcing has taken place. The concern is that appropriate quality and other controls have not been put in place to protect against challenges beyond quality defects – namely malicious influence in the outsourcing process.
  - Increased risk brought through dependency on software-controlled technology. Society, businesses and critical nation-state interests have grown dramatically more reliant on such technology for basic function and survival – even when compared with just a decade ago.
  - Global security environment with numerous security aspects viewed as having a harmful influence on the integrity of supply chains. These aspects include the mode of asymmetrical terror attacks against the interests of stable societies is consistent with cyber terrorism, the electronic interconnectedness of the world enables “triggers” to be pulled from anywhere in the world, and the relative instability of some geographic regions could jeopardise the ability to attain timely technical support for products developed in those areas, should there be a regional problem.

ARECI Report recommends for the European Institutions and Member States to embark on a focused program to promote the integrity of supply chains used to build network systems, and promote the implementation of innovative trust concepts to support the operation of these systems. The program should focus on articulating a vision, providing incentives for research and development, and establishing policies affecting government procurement contract awards.

Related SC27 Efforts – ISO/IEC 27036, Guidelines for Security of Outsourcing

- **Scope**: to define guidance to organizations on the evaluation of security risks involved in the procurement and use of outsourced services. This standard will support the implementation of ISO/IEC 27001/27002 controls for outsourcing and should include the following areas:
  - Strategic goals, objectives and business needs
  - Risks and mitigation techniques
  - Assurance provision

  Note: It is the intent of this standard that outsourcing is ***not limited to ICT outsourcing, but could include other forms of outsourcing*** (e.g. human resources, facilities management) that have information security implications.

ISO/Iec 27036 has a broad scope that addresses outsourcing of any services. However, it excludes products by definition and does not provide an opportunity to specifically address security risks related to ICT outsourcing represented by ICT supply chain security.

Other Related Efforts

- **PC246 and TC247**
  - PC246, *Anti-counterfeiting tools,* is in the process of developing and ISMS-like standard. SC27 has been trying to initiate collaboration (through sending liaison statements) unsuccessfully for some time

- **Internet Security Forum (ISF) proposal –** At the Melaka meeting ISF has proposed a new standard titled ***Information technology – Security techniques – Third Party Information Security Management Standard*** (NWIP N8697)
  - Proposed scope to create the first globally applicable third party information security management standard; address the four key steps in managing one or more third parties: identification and classification; agreement of security arrangements in contracts; validation; and handling exit/contract termination
  - Multipart with Parts 1 and 2 extending ISO/IEC 27001 and ISO/EIC 27002, respectively, for the third party environment
  - ISF was not at the meeting to discuss due to European travel issues

- **Outsourcing Standard NWIP**
  - Submitted by Netherlands in March 2010
  - To provide guidance for the outsourcing of any type of service and/or process and the corresponding resources. This International Standard would cover the entire life cycle of outsourcing and provide a description of the definitions, concepts, and processes that are considered to form good practices in outsourcing
  - Does not address ICT supply chain security but will provide an overarching framework that would help implement ICT supply chain security
  - Proposes a number of liaisons but not with SC27

Study Period Results – Supply Chain Attack Definitions

- SAFECode definition:
  - Compromise of an IT solution by the intentional insertion of malicious code into the solution's software during its development or maintenance. A supply chain attack can be directed at any category of software, including custom software, software delivering a cloud service, a software product, or software embedded in a hardware device. Software in any of these categories is often packaged as a collection of files. To be successful, a software supply chain attack must result in either: a) the modification of an existing software file(s); or, b) the insertion of an additional file(s) into the collection of software files

- PROCENT report definition:
  - Insertion of malicious code, or unintended or reduced functionality, into hardware, software or services during its development, delivery or maintenance
  - Creation of counterfeit hardware, software, systems or services

Conclusions

- Standard is needed to define a common framework for ICT supply chain security, including integrity to help acquirers articulate what they are looking for to suppliers and to help suppliers demonstrate that they have it

- Standard should not repeat content that is already in existence – e.g., lifecycle processes and practices, basic outsourcing and supply chain definitions, security techniques available to improve security of outsourcing (e.g. encryption and code signing)

- Standard should provide:
  - Common set of definitions and concepts
  - Connection to other standard that contain useful techniques and methods to increase ICT supply chain security
  - Specific techniques that will help acquirers and suppliers engage in a useful dialog around ICT products and services acquisition and outsourcing

The ICT supply chain is not homogeneous. Many organizations developed and articulated, from varying points of view, good practices, approaches and technology tools to assure the integrity of their supply chains. Consolidation of this knowledge and these approaches is necessary for progress. (ENISA PROCENT Report)